

# Password Security **Guide**



MetaCompliance®

# Password Security

Passwords are the virtual keys to our digital world, providing access to all our personal accounts, including online banking, email and social media services, as well as all of the data hosted in our cloud storage. Compromised passwords give cybercriminals an open door into these accounts, and the data within.

It is essential that your accounts are available to you, and only you. If your passwords fall into the wrong hands, the consequences, from computer hijacking, identity theft and data breaches, can be severe.

Practising good password hygiene is the best defence against unauthorised access to your devices and personal information. Without having password security best practices top of mind, you leave your organisation open to cyber security threats.



# 15%

According to IBM's 2023 Cost of Data Breach Report, compromised or stolen credentials emerged as one of the primary initial attack vectors, accounting for 15% of breaches in 2023.



# Common Password **Security Threats**

Cybercriminals have several password-hacking tactics at their disposal. **These include:**

## Brute Force

Brute force attacks refer to excessive forceful attempts to gain unauthorised access to a private account. Hackers will use different combinations of characters until the correct combination is found. Longer, more complicated passwords require additional combinations, making them more difficult to crack.



## Dictionary Attacks

Dictionary attacks are a targeted form of brute force attack, whereby hackers run a 'dictionary list' of common words, either from familiar language or typical user passwords, and try these as potential passwords. These attacks are often successful because individuals tend to use simple, easy-to-remember passwords across multiple accounts.



## Phishing

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source.

These emails or text messages often contain a malicious attachment or link leading to a spoofed website.



# Common Password Security Threats



## Password Spraying

Lists of common passwords are used to brute force hack large numbers of accounts. These attacks are successful because, for any given large set of users, there will likely be some who are using common passwords.



## Keystroke Logging

Keystroke logging, or keylogging, involves the installation of malware that monitors and records every keystroke entry made on a device, often without the permission or knowledge of the user.



## Credential Stuffing

Credential stuffing attacks occur when cybercriminals use large amounts of stolen usernames and passwords to fraudulently gain access to user accounts. This information, usually originating from one of many corporate data breaches, is typically obtained on the dark web.





# Password Security Tips

Passwords, when used correctly, are an extremely simple and effective way of protecting your data and systems from unauthorised access. However, many individuals continue to use passwords in a way that exposes them to risk.

By following these tips, you will strengthen the security of your accounts, making it increasingly difficult for potential hackers to obtain unauthorised access.

## Don't Use Personal Information

In this age of social media, we share a lot about ourselves online. Any kind of personal information used as a password can pose a serious threat. A password should never include basic information about yourself, such as the names of relatives, date of birth or pet names.



## Randomise Patterns and Sequences

Your password should never consist of letters only. To make it secure, you should always incorporate a variety of letters, numbers and characters. This may mean using complex abbreviations, writing nonsense phrases, or using a random string of numbers, letters and symbols.

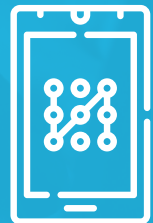


# 39%

**According to Ponemon Institute, 39% of individuals reuse passwords across workplace accounts.**

## Never Reuse Passwords

It can be tempting to use the same password on every account; however, this means that if someone cracks your password on one account, then all your accounts instantly become vulnerable. A unique and different password should be used on each of your accounts to ensure that you remain safe and secure.



# Password Security Tips

## Prioritise Password Length

One of the most important aspects of a strong password is its length. Every character, whether it's a letter, number or symbol, makes your password more difficult to crack. A strong password should be between 12-20 characters long, contain a mix of upper and lowercase letters, and include numbers and/or symbols.



## Never Share Your Password

Password sharing can make it easier for multiple users to access a team account, or for managers to delegate tasks. However, granting account access to unauthorised users can pose substantial security threats to your organisation. You should never share your passwords or write them down.



## Change Your Password Regularly

Using the same password for long stretches of time can increase the risk of a hacker guessing your password and gaining access to your accounts. It is best practice to change your account passwords regularly.



## Use a Password Manager

Many people avoid using different passwords for different accounts because it can be difficult to remember them all. Password managers provide a safe, centralised and encrypted location that keeps a record of all your passwords. Examples of password managers include LastPass, 1Password and Google Chrome's built-in password manager.





# Password Security Tips

## Use Multi-Factor Authentication

Even the strongest password can't protect your account if it gets compromised in a data breach. Two-factor authentication, also known as 2FA, adds an extra layer of security to your online accounts. 2FA prompts users to confirm their identity by inputting a second form of identification.

**There are three types of authentication that can be used to reduce the chance of a hacker fraudulently accessing your account.**



1. **SOMETHING YOU KNOW:** a password, PIN, postcode, or answer to a question, e.g. mother's maiden name.



2. **SOMETHING YOU HAVE:** a token, phone, credit card, SIM or physical security key.



3. **SOMETHING YOU ARE:** biometric data, such as a fingerprint, your voice, or facial recognition.

## Report Password Breaches

Any suspected password breaches must be reported to the IT security team immediately.

